REMARKS

Claims 1-27 are pending in the application. Claims 1-27 were rejected under 35 U.S.C. § 103 (a). Claims 1, 14 and 22 were rejected under 35 U.S.C. § 112.

Rejection Under 35 U.S.C. § 112

Claims 1, 14 and 22 were rejected under 35 U.S.C. § 112, first paragraph, for allegedly failing to comply with the written description requirement.

Applicants respectively traverse this ground of rejection for the following reasons.

Applicants' claim 1 recites,

> "wherein one or more private keys employable for encryption and/or decryption of information are erased via an automatic cutoff of power upon an attempt to move the authentication device;"

Page 12, lines 1-15 of applicants' specification states,

> "The authorization component 208 comprises a power distribution component 604, a private key module 606, and a challenge logic, initialization logic, and durable memory component 608. The power distribution component 604 supplies power to various components of the authorization component 208. For example, the power distribution component 604 supplies power to the private key module 606. The private key module 606 in one example stores one or more private keys and one or more private key identifiers. In one example, the private key module 606 stores the private keys and one or more private key identifiers in volatile memory. In another example, the private key module 606 stores the private keys and one or more private key identifiers in non-volatile memory but erases the private keys upon occurrence a possible security breach. Upon an attempt to move or open the authentication device 104, the power distribution component 604 may cut off power to the private key module 606 to erase the one or more private keys. As a security measure, the power distribution component 604 may cut the power from the private key module 606 to disable the authentication device 104 from processing subsequent requests for authentication."

In other words, the power distribution component is an automated/mechanized means for cutting off power to the private key module 606 to erase the one or more private keys. Power to the private keys is cut off by the power distribution component

upon an attempt to move or open the authentication device. As known by those skilled in the art, automatic, as used in applicants' claims 1, 14 and 22, means "acting or done as if by machine". Thus, the private keys are erased via an automatic, i.e., power distribution component, cutoff of power upon an attempt to move the authentication device. This differs from the cited prior art, Niimura, which discloses that main controller 110 erases key data if main controller 110 determines that the user has turned off the power supply, as stated in column 3, lines 59-65.

Although claims 1, 14 and 22 employ a term, i.e., automatic, that does not appear in the specification, MPEP 1302.01 states that the exact terms do not have to be used to satisfy the written description requirements of the first paragraph of 35 U.S.C. 112. 37 CFR 1.121(e) merely requires substantial correspondence between the language of the claims and the language of the specification.

In view of the foregoing, applicants assert that the rejection under 35 U.S.C. § 112, first paragraph has been overcome.

Rejection Under 35 U.S.C. § 103 (a)

Rejection Under Karaoguz, MacKenzie, Niimura and Williams

Claims 1-6, 8-18 and 20-27 were rejected under 35 U.S.C. § 103 (a) as being unpatentable over U. S. Patent Application Number 2004/0059914 issued to Karaoguz dated March 25, 2004 in view of U. S. Patent Application Number 2002/0141594 A1 issued to MacKenzie dated October 3, 2002, and further in view of U. S. Patent Number 7,420,596 issued to Niimura on September 2, 2008, and further in view of U. S. Patent Number 7,139,920 issued to Williams on November 21, 2006.

Applicants respectively traverse this ground of rejection for the following reasons.

First, applicants' claim 1 recites,

> "an authentication device that authenticates a computing device, in communication with the authentication device, through employment of a determination that a current location of the authentication device matches an initial location of the authentication device;
>
> wherein one or more private keys employable for encryption and/or decryption of information are erased via an automatic cutoff of power upon an attempt to move the authentication device."

As stated in the Final Office Action, the proposed combination of Karaoguz, MacKenzie and Niimura does not teach or suggest "wherein one or more private keys employable for encryption and/or decryption of information are erased via an automatic cutoff of power upon an attempt to move the authentication device", as recited in applicants' claim 1.

Applicants agree that Williams discloses a power supply unit with an automatic cut-out. However, the automatic cut-out is triggered to protect the power supply unit from damage caused by excess power drain, i.e., a fail-safe or back-up protection facility for the power supply unit, rather than to erase private keys upon an attempt to move the authentication device as required by applicants' claim 1. See column 4, lines 21-30. Thus, Williams, similar to Karaoguz, MacKenzie and Niimura, is missing the "wherein one or more private keys employable for encryption and/or decryption of information are erased via an automatic cutoff of power upon an attempt to move the authentication device" elements, as recited in applicants' claim 1.

Second, the Final Office Action suggests that there is a motivation to combine Karaoguz, MacKenzie and Niimura with Williams —namely, to yield predictable results. However, applicants respectfully submit that the teachings in Karaoguz, Mackenzie, Niimura and Williams provide no basis to conclude that a person of ordinary skill in the art would use Mackenzie's, Niimura's and Williams' techniques to facilitate Karaoguz's arrangement to arrive at the subject matter of applicants' claim 1, so the combination is improper.

Specifically, each reference addresses a problem so different from the one addressed by the other references that the respective teachings provide no motivation for the person of ordinary skill to combine them.

More specifically, Karaoguz addresses the problem of authenticating and confirming an identity of a user based on the distance range location information and/or the geographic position location information of the user's wireless device. In Karaoguz, the problem is addressed by receiving a request message from a sender to access a resource provided through a wireless network; determining first signal-generated location information of the sender; identifying the sender using the first signal-generated

location information; confirming an identity of the sender; and authorizing access for the sender to access the resource.

By contrast, Mackenzie addresses the problem of providing techniques by which a networked cryptographic device can be immunized to offline dictionary attacks in case the device is captured. In Mackenzie, the problem is addressed by generating in a first party device a request for the partial assistance of a device associated with a second party in recovering a key from data stored on the first party device, wherein the second party device is remote from the first party device; transmitting the request from the first party device to the second party device; receiving results in the first party device generated by the second party device based on the partial assistance provided by the second party device; and using at least a portion of the received results in the first party device to recover the key for subsequent use as a private key in one or more associated public key cryptographic techniques.

Niimura addresses the problem of generating image data and authentication data of the image data. In Niimura, the problem is addressed by an image sensing unit that generates image data of a sensed image; and a key data control unit that (a) generates key data if a user turns on the power of the image sensing apparatus, and (b) erases the key data from the image sensing apparatus if a user turns off the power of the image sensing apparatus, wherein the key data is used to generate authentication data, and the authentication data is used to authenticate whether the image data is altered,

Rather than addressing problems that involve a) providing authenticating and confirming an identity of a user based on the distance range location information and/or the geographic position location information of the user's wireless device as done by Karaoguz or b) providing techniques by which a networked cryptographic device can be immunized to offline dictionary attacks in case the device is captured as done by Mackenzie, or c) generating image data and authentication data of the image data as done by Niimura, it appears that the problem being addressed by Williams is the need to allow power supplies in computers to better cope with variations in power demand. In Williams, the problem is addressed by a power supply unit operable to provide power to at least one electronic component, said power supply unit having a detector which is responsive to an increase in level of power output from the power supply unit beyond a

predetermined limit to initiate transmission of an alert signal to the at least one electronic component, wherein said alert signal is set to one of a plurality of values, and wherein said plurality of alert values comprises two or more values each representing a respective alert condition and one value representing a normal condition.

Also, each reference addresses devices so different from the devices addressed by the other references that the respective teachings provide no motivation for the person of ordinary skill to combine them.

Karaoguz addresses wireless communication devices. MacKenzie addresses networked cryptographic devices. Niimura addresses digital cameras. By contrast, Williams addresses computers.

Accordingly, one of ordinary skill in the art would **not** be motivated to combine a solution that provides 1) receiving a request message from a sender to access a resource provided through a wireless network; determining first signal-generated location information of the sender; identifying the sender using the first signal-generated location information; confirming an identity of the sender; and authorizing access for the sender to access the resource, with 2) generating in a first party device a request for the partial assistance of a device associated with a second party in recovering a key from data stored on the first party device, wherein the second party device is remote from the first party device; transmitting the request from the first party device to the second party device; receiving results in the first party device generated by the second party device based on the partial assistance provided by the second party device; and using at least a portion of the received results in the first party device to recover the key for subsequent use as a private key in one or more associated public key cryptographic techniques, with 3) an image sensing unit that generates image data of a sensed image; and a key data control unit that (a) generates key data if a user turns on the power of the image sensing apparatus, and (b) erases the key data from the image sensing apparatus if a user turns off the power of the image sensing apparatus, and 4) a power supply unit operable to provide power to at least one electronic component, said power supply unit having a detector which is responsive to an increase in level of power output from the power supply unit beyond a predetermined limit to initiate transmission of an alert signal to the at least one electronic component.

Furthermore, Karaoguz makes no mention of a power supply unit with an automatic cut-out nor is there a teaching in Karaoguz to suggest that there would be an improvement in Karaoguz's technique with a power supply unit with an automatic cut-out. Since the teachings of Karaoguz adequately address the problem of authenticating and confirming an identity of a user based on the distance range location information and/or the geographic position location information of the user's wireless device, there is no motivation to combine Karaoguz, Mackenzie and Niimura with Williams' teachings. Given that Karaoguz's technique does **not** suffer from the problems that Williams addresses, one of ordinary skill in the art would **not** be led to try to improve Karaoguz's technique with Williams' teachings.

Thus, one of ordinary skill in the art would **not** be motivated to modify Karaoguz with Mackenzie's, Niimura's and Williams' teachings. Consequently, applicants respectfully submit that the Examiner is relying on the use of impermissible hindsight in an attempt to reconstruct applicants' teachings by combining Karaoguz, Mackenzie, Niimura and Williams. Accordingly, applicants submit that the combination and resultant rejection are improper.

Therefore the proposed combination of Karaoguz, MacKenzie, Niimura and Williams does **not** teach or suggest all of the limitations in applicants' claim 1, and therefore claim 1 is allowable over the proposed combination. Since claims 2-13 and 23-27 depend from allowable claim 1, these claims are also allowable over the proposed combination.

Independent claims 14 and 22 each have a limitation similar to that of independent claim 1, which was shown is **not** taught by the proposed combination of Karaoguz, MacKenzie, Niimura and Williams. For example, claims 14 and 22 recite, "wherein one or more private keys employable for encryption and/or decryption of information are erased via an automatic cutoff of power upon an attempt to move the authentication device". The proposed combination of Karaoguz, MacKenzie, Niimura and Williams does **not** teach or suggest this limitation for the above-mentioned reasons. Therefore, claims 14 and 22 are likewise allowable over the proposed combination. Since claims 15-21 depend from claim 14, these dependent claims are also allowable over the proposed combination.

Rejection Under Karaoguz, MacKenzie, Niimura, Williams and Wheeler

Claims 7 and 19 were rejected under 35 U.S.C. § 103 (a) as being unpatentable over Karaoguz in view of MacKenzie, and further in view of Niimura, and furthermore in view of Williams, and furthermore in view of U. S. Patent Application Number 2007/0088950 issued to Wheeler dated April 19, 2007.

Applicants respectfully traverse this ground of rejection for the following reasons.

This rejection is based on the rejection under Karaoguz, MacKenzie, Niimura and Williams being proper. As that ground of rejection has been overcome, and none of the cited references teach or suggest "wherein one or more private keys employable for encryption and/or decryption of information are erased via an automatic cutoff of power upon an attempt to move the authentication device" as recited in applicants' independent claims 1, 14 and 22, the proposed combination of Karaoguz, MacKenzie, Niimura, Williams and Wheeler does **not** supply this missing element. Thus, this combination does **not** make obvious any of applicants' claims, all of which require the aforesaid limitation.

Conclusion

It is respectfully submitted that the Office Action's rejections have been overcome and that this application is now in condition for allowance. Reconsideration and allowance are, therefore, respectfully solicited.

In view of the above amendments and remarks, allowance of all claims pending is respectfully requested. If a telephone conference would be of assistance in advancing the prosecution of this application, the Examiner is invited to call applicants' attorney.

Respectfully submitted,

James Milton
Attorney for Applicants
Reg. No. 46,935

Dated: April 16, 2009

PATTI, HEWITT & AREZINA, LLC
Customer Number 47382